IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

UNITED STATES OF AMERICA Plaintiff, v. $1,098,699.64 IN UNITED STATES CURRENCY Defendant.	§ § § § § § § §	NO: 6:24-cv-00030

AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Brad Schley, after being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Senior Special Agent (SSA) with the United States Secret Service (USSS) and have been so employed since September 2001. During my tenure with the Secret Service, I have been assigned to investigate violations of federal laws, including violations of Title 18 of the United States Code, specifically those related to the passing of counterfeit United States currency, money laundering, and wire fraud. I received criminal investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland, pertaining to criminal investigations of counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. During my employment with the USSS, I have conducted investigations resulting in the arrest of suspects and seizures of criminally derived property. I am an investigative and law

enforcement officer of the United States, in that I am empowered by law to conduct investigations and to make arrests for felony offenses, under authority of 18 U.S.C. § 3056.

2. The statements contained in this affidavit are based in part upon my experience, my knowledge of the facts and circumstances surrounding this investigation, and on information provided to me by other law enforcement personnel and other witnesses.

PROPERTY FOR FORFEITURE

3. This Affidavit is made in support of a civil forfeiture complaint concerning the following personal property:

a. $73,213.53 in JP Morgan Chase (JPMC) Bank account 000000000005013382181 (TARGET ACCOUNT 1);

b. $491,255.11 in JPMC Bank account 00000000000530558678 (TARGET ACCOUNT 2);

c. $5,723.41 in JPMC account 00000000000525987330 (TARGET ACCOUNT 3);

d. $528,507.59 in JPMC account 00000000000918258267 (TARGET ACCOUNT 4);

that totals $1,098,699.64 into Check No. 4557154754 and was seized on or about November 2, 2023, in Tyler, Texas pursuant to a seizure warrant.

LEGAL AUTHORITY FOR FORFEITURE

4. The funds to be forfeited represent proceeds of a fraudulent cryptocurrency investment scheme that often utilizes spoofed domains. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal. In particular, the unknown scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to United States-based victims, including victims in Tyler, Texas, which is located within the Eastern District of Texas. Scammers then fooled victims into "investing" in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal the victims' money.

5. This type of scam is often identified as "pig butchering" (derived from the Chinese phrase, which is used to describe this scheme) and involves scammers spending significant time getting to know, targeting and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds through a provided BTC, USDT, ETH or USDC deposit address, and are further told they can expect to make a sizeable return on their

investments. As initial smaller investments are made, the spoofed websites falsely display a significant increase in the victim's account balance, which entices the victim to continue making investments, which typically end with a final large deposit or transaction. When the victim attempts to make a withdrawal, the scammers attempt to coerce the victims to make additional investments. These tactics can include requesting additional investments due to "significant profits" gained on the account or other reasons such as freezing the account due to "taxes owed" or "suspicious behavior." Regardless of how the scammers attempt to solicit additional investments from the victims, the victims are unable to retrieve any portion of their investment.

6. I believe the above-listed property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because the property was involved in or traceable to property involved in money laundering in violation of 18 U.S.C §§ 1956 or 1957, or constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)).

7. Any property, real or personal, which was involved in a transaction in violation of 18 U.S.C. §§ 1956 or 1957 or any property traceable to such property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

8. 18 U.S.C. § 1956 (a)(1) makes it a crime to knowingly conduct or attempt to conduct a "financial transaction" with proceeds from "specified unlawful activity"

(SUA) with specific intent to: promote the SUA, conceal or disguise the source, origin, nature, ownership, or control of the proceeds; or evade reporting requirements.

9. The purpose of "money laundering" as defined by 18 U.S.C. § 1956 is to disguise illicit nature of funds by introducing it into legitimate commerce and finance thereby making them "clean." This financial process is most commonly conducted using three steps referred to as "placement," "layering," and "integration." Typically, the "placement" phase of this financial process takes place when proceeds from illicit sources are placed in a financial institution or business entity. "Layering" takes place when these funds are then used in seemingly legitimate commerce transactions which makes the tracing of these monies more difficult and removed from the criminal activity from which they are a source. Finally, the "integration" phase is when these funds are then used to promote the unlawful activity or for the personal benefit of the money launderers and others.

10. I also have probable cause to believe that this property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because the property constitutes or is derived from proceeds traceable to violations of 18 U.S.C. § 1343 or a conspiracy to commit such offense (18 U.S.C. § 1349). Wire fraud is an SUA. 18 U.S.C. § 981(a)(1)(C).

11. Any property, real or personal, which constitutes proceeds or is derived from proceeds traceable to a violation of 18 U.S.C. §§ 1343 or 1349 is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

12. Under 18 U.S.C. § 984, for any forfeiture action in rem in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;

b. It is not a defense that those funds have been removed and replaced by other funds; and

c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

13. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the "guilty" property had been kept.

FACTS SUPPORTING FORFEITURE

14. The United States is investigating a pig butchering scheme involving a fraudulent cryptocurrency investment scheme that utilizes spoofed domains. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud),

18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud), and 18 U.S.C. §§ 1956 and 1957 (Laundering of Monetary Instruments).

15. The case involves the laundering of proceeds obtained from victims of the fraudulent scheme. Part of the money laundering scheme was to funnel proceeds from pig butchering victims through the various business accounts to accounts located abroad. One business, identified as Elights Trading Inc., held a bank account that served as a funnel account and received fraud proceeds from bank accounts held in the names of the pig butchering victims. The Elights Trading Inc. bank account was provided to victims located within the Eastern District of Texas as a means in which they would pay their "taxes and/or fees" concerning their "earnings" as part of this scheme.

16. Investigators interviewed multiple victims who sent funds to the Citibank held in the name of Elights Trading. In summary, these victims reported to have been tricked into believing they were investing in cryptocurrency, when in fact they were provided with links or information leading them to use spoofed domains or applications of legitimate cryptocurrency exchanges. One of these victims was identified as T.G.

Victim T.G.

17. Investigators interviewed victim T.G. regarding the $230,000 transaction remitted to the ELIGHTS TRADING Account. T.G. met a friend on Facebook in or about May 2023, but has never met this individual face to face. T.G.'s new female friend portrayed herself as being very wealthy and T.G. inquired how he could invest money to

earn a large and safe return. T.G.'s friend provided a link to Telegram where T.G. was led to believe he was working with employees of OKEX, a cryptocurrency exchange. T.G. received instructions via Telegram regarding investments, including the information for the ELIGHTS TRADING account. T.G. believed he was purchasing options in cryptocurrency and not specific cryptocurrency coins such as Bitcoin. T.G. has invested approximately $850,000 in total by sending to other bank accounts he received from the OKEX Telegram communications. T.G. has only requested small withdrawals from his investment and has received only a few thousand dollars and has not made any large withdrawal requests.

18. T.G. informed USSS investigators that during this scheme, he was provided the JPMC Bank account in the name of SUNSHINES TRADING, account number ending in 2181, TARGET ACCOUNT 1. A review of JPMC Bank records pertaining to this account reflect T.G. sent $80,000 to this account on September 20, 2023.

TARGET ACCOUNT INFORMATION AND TRANSACTIONS

19. Investigators issued a Federal Grand Jury subpoena to JPMC and obtained the bank records for the JPMC Bank accounts in the name of SUNSHINES TRADING INC., account number ending in 2181 (TARGET ACCOUNT 1); and account number ending in 8678 (TARGET ACCOUNT 2); the account held in the name of Qi Sun account number ending in 7330 (TARGET ACCOUNT 3); and the account held in the name of MAGIC LOCATION TRADING LLC ending 8267 (TARGET ACCOUNT 4).

These bank records identified the signor on TARGET ACCOUNTS 1 AND 2 as Qi Sun. The records indicate that on or about August 9, 2023, Qi Sun opened the business bank account identifying SUNSHINES TRADING INC. as a corporation. The records reflect that SUN provided the business address of 2124 Las Lomitas Drive, Hacienda Heights, California.

20. USSS investigators conducted surveillance of the residence located at 2124 Las Lomitas Drive, Hacienda Heights, California. USSS investigators identified this location in a residential-only neighborhood and is equipped with a private driveway with a gate. USSS investigators were unable to discover any business activity at this location during their surveillance.

21. Investigators were unable to locate an Internet business presence for Sunshines Trading Inc. or Magic Location Trading LLC.

22. Analysis of the bank records for TARGET ACCOUNT 1 indicate the following wire deposits were made into TARGET ACCOUNT 1 totaling $346,264.67:

DATE	AMOUNT	VICTIM
9/15/2023	$55,750.00	A.V.V.
9/18/2023	$10,000.00	R.C.
9/19/2023	$10,000.00	H.T.N
9/20/2023	$30,000.00	C.W.V.
9/20/2023	$80,000.00	T.G.
9/21/2023	$15,168.00	T.W.
9/21/2023	$45,000.00	T.E.
9/25/2023	$20,000.00	H.C.
9/25/2023	$20,100.00	B.A.J.
9/26/2023	$20,015.00	M.S. Sr
9/27/2023	$10,000.00	P.B. / R.B.

9/27/2023	$30,231.67	A.Y.S.

INTERVIEWS OF ADDITIONAL VICTIMS THAT SENT FUNDS TO TARGET ACCOUNT 1

23. In addition to victim T.G., Investigators interviewed additional victims who were identified as having sent funds to TARGET ACCOUNT 1 as a result of a cryptocurrency investment fraud scheme.

Victim R.C.

24. USSS investigators identified and interviewed victim R.C. regarding the $10,000 transaction he sent to TARGET ACCOUNT 1 on or about September 19, 2023. R.C. stated he met an acquaintance online in August 2023 who befriended R.C. R.C. stated he communicated daily via text message with the unknown subject who utilized number 213.778.1166. R.C. is 65 years of age and does not know how to invest in cryptocurrency which enabled the fraudster to assist R.C. with opening an account at Crypto.com. R.C. stated Crypto.com closed his account.

25. R.C.'s initial investments were in small increments, $1,000 to $2,000 at a time. R.C.'s investments continued to increase in value and he was enticed to invest more funds. R.C. explained how the unknown subject provided him with the account information for TARGET ACCOUNT 1, where he sent $10,000. On or about October 12, 2023, R.C. attempted to withdraw his funds and was advised he would need to pay taxes. R.C. he informed the unknown subject that he would withdraw the funds and pay his taxes through his CPA. The unknown subject told R.C. that the taxes were to be paid

prior to any funds being returned. R.C. realized at this point he was involved in a scam and suffered a loss of approximately $32,000.

26. Based on my training and experience conducting fraud investigations involving cryptocurrency, legitimate exchanges such as Crypto.com will often close a customer's account when the customer's transactions are sent to wallets and/or addresses that have been previously reported for fraud.

Victim R.B.

27. USSS investigators identified and interviewed victim R.B. regarding the $10,000 transaction he sent to TARGET ACCOUNT 1. R.B. met a female online that used the name Annie Rybka. R.B. was unfamiliar with investing in crypto currency and Rybka referred him to a platform at spreadex.com and/or spreadexs.com, where he was made to believe is $10,000 investment has appreciated to approximately $13,000. R.B. was able to withdraw and receive $2,500 of his funds back into his account, but he has yet to recover any additional funds.

Victim A.Y.S.

28. USSS investigators identified and interviewed victim A.Y.S. regarding the $30,231.67 transaction he sent to TARGET ACCOUNT 1. A.Y.S. was contacted by a wrong number text via WhatsApp by someone using the name Katy LNU. A.Y.S. said that Katy LNU claimed to have learned how to earn money investing in cryptocurrency while in college. A.Y.S. admitted that in addition to sending funds to Sunshines Trading,

he also sent funds to what he believed was his cryptocurrency account from Crypto.com and Coinbase.com. A.Y.S. has sent a total of approximately $227,000 as a result of this scheme, and stated his cryptocurrency wallet was adjusted to reflect a value of over $1.1m. A.Y.S. stated the domains his cryptocurrency wallet continued to change and included: deiarng.co, maniesp.co, moreasn12.co, usenba02.co, donaeion.co and foecum.co.

29. A.Y.S. informed USSS investigators he attempted to withdraw funds from his cryptocurrency account and was informed that he needed to pay commission fees and other fees prior to being able to withdraw any of his funds. A.Y.S. has been paying fees and has yet to get access to his account because the fraudsters continue to inform him of the need to pay additional fees. A.Y.S. stated that on October 25, 2023, he sent approximately $11,000 as part of the requested fees to a bank account at Standard Charter Bank in Hong Kong, a bank which has been used frequently by fraudsters in this investigation.

INVESTIGATION IDENTIFIES TARGET ACCOUNT 2 AS RECEIVING VICTIMS' FUNDS

30. In addition to TARGET ACCOUNT 1, USSS investigators identified TARGET ACCOUNT 2 was also held in the name of Sunshines Trading Inc. USSS investigators reviewed the bank records for TARGET ACCOUNT 2 and discovered that this account was also utilized to receive funds from victims of this cryptocurrency investment fraud scheme.

31. Analysis of the bank records for TARGET ACCOUNT 2 indicate the following wire deposits were made into TARGET ACCOUNT 2 totaling $2,396,514.90.

TRANSACTION DATE	TRANSACTION AMOUNT	VICTIM
8/28/2023	$22,492.90	D.J.R.
8/29/2023	$10,000.00	D.C.L.
8/31/2023	$39,990.00	L.T.
8/30/2023	$17,600.00	J.R.O
8/31/2023	$10,000.00	B.T.W.
8/30/2023	$10,000.00	R.C.
8/25/2023	$90,000.00	A.Z.B.
8/29/2023	$10,000.00	C.A.B.
8/25/2023	$20,000.00	S.E.K.
8/24/2023	$10,000.00	D.M.
8/31/2023	$45,000.00	A.V.V.
8/28/2023	$80,000.00	B.H.
8/24/2023	$50,000.00	C.G.D.
8/25/2023	$121,500.00	J.L.B.
8/30/2023	$20,000.00	S.J.M.
8/24/2023	$10,020.00	F.E.F.
8/31/2023	$25,000.00	J.J.B.
8/31/2023	$210,000.00	A.Z.B. 2nd transaction
9/5/2023	$8,500.00	J.C.K.
9/25/2023	$402,310.00	T.J.S.
9/12/2023	$10,000.00	G.S.M.
9/27/2023	$120,000.00	F.J.S.
9/5/2023	$49,989.00	L.T. 2nd transaction
9/26/2023	$20,000.00	J.B.S.
9/12/2023	$85,000.00	R.M.
9/25/2023	$80,000.00	F.J.S. JR
9/5/2023	$150,000.00	G.M.
9/5/2023	$10,000.00	R.J.L.
9/27/2023	$30,000.00	T.L.C.
9/27/2023	$57,348.00	C.T.C.
9/25/2023	$5,000.00	H.H.M.
9/11/2023	$18,735.00	M.G.
9/1/2023	$10,000.00	J.B.S. 2nd transaction
9/12/2023	$400,000.00	B.S.W.
9/27/2023	$40,000.00	R.E.M.

9/27/2023	$30,030.00	N.N.C.
9/12/2023	$40,000.00	T.H.L.
9/27/2023	$28,000.00	R.A.N.

INTERVIEWS OF VICTIMS WHO SENT FUNDS TO TARGET ACCOUNT 2

Victim B.S.W.

32. USSS investigators identified and interviewed victim B.S.W. regarding the $400,000.00 transaction he sent to TARGET ACCOUNT 2. B.S.W. was contacted by Edith Webb on LinkedIn. B.S.W. explained how Webb introduced him to a platform, Black Rock, that she advertised and demonstrated how she was investing in silver and gold. B.S.W. claimed Webb advertised to him that she was earning a large return on her investment in a short timeframe and it enticed B.S.W. to invest. Based on Webb's information, B.S.W. expected to earn a return of approximately 25%. B.S.W. recently discovered his Black Rock account was inaccessible and he could not retrieve funds from his account without paying for fees and/or taxes.

Victim T.H.L.

33. USSS investigators identified and interviewed victim T.H.L. regarding the $40,000.00 transaction he sent to TARGET ACCOUNT 2. T.H.L. he met a person using the name Susan Davis on Facebook in or about March 2023. T.H.L. explained how Davis introduced him to a domain known as Ant/web3, an investment platform she utilized and demonstrated to T.H.L.. Based on Davis's use and demonstration of this platform, T.H.L. was made to believe he would receive a large return on his investment.

T.H.L. invested approximately $90,000 in Ant/web3. T.H.L. recently attempted to make a withdrawal of his funds from the Ant/web3 account, and he was informed he would need to pay approximately $47,095.20 to remove the abnormal activity on his account, which included a "deposit" made by Davis. T.H.L. deleted the contact information for Davis since he learned she was the person who caused him to lose a large amount of funds.

34. Based on my training and experience conducting fraud investigations, fraudsters controlling these domains and can manipulate the data in the domain, to include the "account balance" and make it appear as if there was a deposit or gain in the victim's "account."

Victim R.A.N.

35. USSS investigators identified and interviewed victim R.A.N. regarding the $28,000.00 transaction he sent to TARGET ACCOUNT 2. R.A.N. met someone using the name Cindy Smith via Facebook in or about August 2023. R.A.N. explained how Smith introduced him to Curve Financial, an investment platform Smith advertised as using successfully to invest in cryptocurrency. As a result of Smith's advertisement and demonstrations in using Curve Financial, R.A.N. was made to believe he would earn 20-30% on his investment of approximately $245,000.

36. R.A.N. provided USSS investigators images of bank account information domiciled in Vietnam that he was instructed to send funds to when funding his Curve

Financial account. R.A.N. also provided USSS investigators an image of a California driver's license bearing the name Cindy Smith, driver's license number D5265043. USSS analysts queried law enforcement databases and confirmed the aforementioned driver's license is fictitious, as the driver's license number is assigned to a person with a completely different name and date of birth.

37. The bank account provided to R.A.N. was in the name of Neil Company Limited, a different name than Curve Financial.

38. R.A.N. attempted to withdraw his funds and was informed he needed to pay $77,450 in order to receive his funds. R.A.N. said the fraudsters from Curve Financial were insistent on the necessity to send these funds to a foreign trader.

INVESTIGATION IDENTIFIES TARGET ACCOUNT 3 AS RECEIVING VICITM'S FUNDS

39. USSS investigators reviewed records obtained from JPMC Bank which identified TARGET ACCOUNT 3 as a personal account for Qi Sun, the signor for TARGET ACCOUNTS 1 and 2. The bank records reflect TARGET ACCOUNT 3 received minimal wire transactions. One wire transaction was received from reported victim S.N. in the amount of $102,460.00. The records indicate these funds were transferred to TARGET ACCOUNT 2.

INVESTIGATION IDENTIFIES TARGET ACCOUNT 4 AS RECEIVING VICTIMS' FUNDS

40. During an investigation of Zheng Lin, USSS investigators discovered Lin was the signor on TARGET ACCOUNT 4, in the name of Magic Location Trading LLC.

41. USSS investigators reviewed IC3 reports submitted by individuals who sent funds to TARGET ACCOUNT 4 as part of the fraudulent cryptocurrency investment scheme. The individuals reported to IC3 similar circumstances as other victims that sent funds to TARGET ACCOUNT 4. The IC3 reports dated June 5, 2023 to September 22, 2023 indicate that four separate individuals sent funds to TARGET ACCOUNT 4 totaling approximately $80,000.

42. USSS investigators obtained the JP Morgan Chase bank records for TARGET ACCOUNT 4 via a federal grand jury subpoena. A review of these records indicated TARGET ACCOUNT 4 received the following transactions from the noted victims totaling approximately $2,936,719.08:

DATE	TRANSACTION AMOUNT	VICTIM
6/30/2023	$15,000.00	S.W.G.
6/30/2023	$12,880.70	E.S.C.
6/30/2023	$15,500.00	B.D.M
7/3/2023	$3,000.00	F.X.M.
7/3/2023	$10,000.00	H.C.C.
7/5/2023	$30,000.00	Y.T.
7/5/2023	$15,000.00	H.C.C.
7/5/2023	$112,000.00	X.Y.L.
7/6/2023	$10,000.00	C.A.K.
7/6/2023	$4,000.00	R.R.
7/6/2023	$5,000.00	F.L.

7/24/2023	$15,000.00	J.E.S. Sr
8/11/2023	$47,000.00	I.T.
8/23/2023	$10,000.00	S.A.C.
8/23/2023	$120,000.00	L.P.
8/24/2023	$61,000.00	D.R.
8/29/2023	$7,166.00	T.K.
8/29/2023	$14,530.00	J.M.A.
8/31/2023	$10,000.00	K.B. TSTEE/GRNT
9/1/2023	$15,000.00	Y.C.C.
9/1/2023	$45,000.00	F.L.F. III
9/1/2023	$65,000.00	F.L.F. III
9/1/2023	$90,000.00	R.N.
9/5/2023	$13,000.00	D.A.D.
9/5/2023	$25,000.00	D.G.E.
9/5/2023	$100,000.00	C.A.L.
9/5/2023	$20,050.00	J.A.P.
9/5/2023	$20,000.00	G.P.M JR
9/6/2023	$80,765.20	A.MA.
9/6/2023	$10,000.00	N.K.S.
9/8/2023	$20,155.18	M.C.I.
9/11/2023	$329,721.00	L.P.
9/11/2023	$250,000.00	T.D.
9/12/2023	$25,000.00	P.K.N
9/13/2023	$100,000.00	R.S.L.
9/14/2023	$100,000.00	S.T.K.
9/14/2023	$153,000.00	G.J.S.
9/15/2023	$152,000.00	R.N.
9/18/2023	$179,350.00	M.G.F.
9/19/2023	$100,000.00	S.J.T.
9/19/2023	$349,000.00	J.J.P
9/21/2023	$15,500.00	U.W.
9/21/2023	$10,000.00	K.J.B.
9/21/2023	$50,000.00	E.K.
9/22/2023	$52,100.00	T.L.R.
9/22/2023	$20,001.00	S.S.A.
9/22/2023	$10,000.00	M.A.P.
9/22/2023	$20,000.00	J.B.T.

INTERVIEWS OF ADDITIONAL VICTIMS THAT SENT FUNDS TO TARGET ACCOUNT 4

43. USSS Investigators interviewed victims who were identified as having sent funds to TARGET ACCOUNT 4 as a result of a cryptocurrency investment fraud scheme.

Victim J.M.A.

44. USSS investigators identified victim J.M.A. regarding the $14,530.00 transaction he sent to TARGET ACCOUNT 4. J.M.A. acknowledged his transaction was part of a cryptocurrency investment fraud scheme. J.M.A. described the situation regarding his involvement and these circumstances are very similar to what other victims of this fraud scheme have reported. J.M.A. met an unknown subject on Facebook and their conversations eventually turned to investments into cryptocurrency. J.M.A. communicated with the unknown subject who used WhatsApp 724.862.1331.

45. J.M.A. was provided a domain or ap referred to as Nutex, and made a few small investments when they grew rapidly. J.M.A. was able to withdraw approximately $1,500 early in his investment. J.M.A.'s Nutex account appeared to grow at a rapid pace and he was enticed to invest more funds. J.M.A. claimed to have invested a total of approximately $30,000 as part of this scheme. J.M.A. is a retired attorney.

Victim D.G.E.

46. USSS investigators identified and interviewed victim D.G.E. regarding the $25,000.00 transaction he sent to TARGET ACCOUNT 4. D.G.E. was contacted in July

2023 by a subject using the name Sofia Buterin, during a wrong number call or text. D.G.E. continued to communicate with Buterin via text and WhatsApp. D.G.E. received photographs of Buterin and also facetimed or video called with Buterin. D.G.E. stated the individual in the photos sent by Buterin matched the person he video called. D.G.E. invested approximately $80k as part of this investment fraud scheme and was informed that he would be able to earn a return of up to $1m within a few months of investing.

47. D.G.E. provided screen shot images of a Telegram chat from Buterin who provided domain https://t.me/telecoincss and a link noted as "Telegram Coin Beta4.1." An image of a financial transaction was also provided, detailing $25,000 on 09/14/23 was sent to Hang Seng Bank LIMI, beneficiary Chen Rucai.

48. USSS investigators identified the name Sofia Buterin as a name previously reported by victim K.S. who sent funds to the suspect bank account of Elights Trading.

49. Elights Trading is the same entity in this fraud scheme that EDTX victims K.J. and H.J. were provided to pay their taxes as part of this scheme.

Victim M.C.I.

50. USSS investigators identified and interviewed M.C.I. regarding the $20,155.18 transaction he sent on September 8, 2023 to TARGET ACCOUNT 4. M.C.I. acknowledged the transaction was as a result of a fraudulent cryptocurrency investments scheme. M.C.I. met an unknown subject on the Internet in October 2022 who also

claimed to be from China. M.C.I. stated he communicated with the unknown subject using the Line ap and was persuaded to invest in cryptocurrency via a Meta domain or ap.

51. M.C.I. was made to believe he would receive a return of approximately 20% if he invested using the Meta domain or ap. Over the course of several smaller transactions, M.C.I. has invested approximately $50,000. When M.C.I. attempted to withdraw the funds, he was informed he needed to pay taxes prior to withdrawing any funds. As a result, M.C.I. sent an additional $50,000 to pay taxes and fees. M.C.I. stated his Meta account has been deleted, and has not been able to access any of his funds.

TARGET ACCOUNT TRANSACTION ACTIVITY FOR ALL TARGET ACCOUNTS

52. Investigators obtained bank records regarding TARGET ACCOUNT 1 and discovered that between September 12, 2023 to September 28, 2023, the withdrawal activity included bank fees and ten outgoing wire transactions. These wire transactions were sent to financial institutions in China and Singapore totaling $2,471,740.00.

53. USSS investigators obtained bank records regarding TARGET ACCOUNT 2 and discovered outgoing wires were sent to China ($198,000.00), Hong Kong ($357,048.00) and domestic accounts held in the names of Paretone Capital Limited ($1,683,073.00). The time period for these transactions were August 21, 2023 to September 28, 2023.

54. USSS investigators obtained bank records regarding TARGET ACCOUNT 4 and discovered that between July 2023 to August 2023, TARGET ACCOUNT 4 sent at

least 7 wire transfers to Standard Chartered Bank and other financial institutions in Hong Kong totaling at least $1,268,785.00.

55. The records for the TARGET ACCOUNTS also indicate the recent victims sent a total of $5,781,958.65 to the TARGET ACCOUNTS during the time period of on or about June 30, 2023 – September 28, 2023.

56. During this time period, there were no identifiable normal business transactions such as payroll, utilities or other operational expenses for Sunshines Trading or Magic Location Trading.

57. Based on my training and experience, fraudsters will obtain business bank accounts to receive funds from victims based in the United States and rapidly move funds to places outside of the United States to avoid detection and seizure by law enforcement officers. This activity coupled with the rapid movement of funds reflected in the transaction history of the TARGET ACCOUNTS points to money laundering activity that is common in these fraud schemes.

58. On or about October 3, 2023, investigators provided a freeze letter request to JPMC Bank for assets and monies in the **TARGET ACCOUNTS** to be frozen.

59. On or about November 2, 2023, USSS investigators obtained and served a federal seizure warrant for any and all funds held in the **TARGET ACCOUNTS.**

60. On or about November 14, 2023, USSS investigators received a JPMC Bank cashier's check bearing number 4557154754 that was drawn on the **TARGET ACCOUNTS** in the amount of $1,098,699.64.

CONCLUSION

61. I submit that this affidavit supports probable cause for a warrant to forfeit all funds, monies, and other things of value up to $1,098,699.64 seized from JPMC Bank accounts:

a. $73,213.53 in JP Morgan Chase (JPMC) Bank account 000000000005013382181 (TARGET ACCOUNT 1);

b. $491,255.11 in JPMC Bank account 00000000000530558678 (TARGET ACCOUNT 2);

c. $5,723.41 in JPMC account 00000000000525987330 (TARGET ACCOUNT 3);

d. $528,507.59 in JPMC account 00000000000918258267 (TARGET ACCOUNT 4);

62. Based on my experience and the information herein, I have probable cause to believe that the seized $1,098,699.64 constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)), are traceable to a money laundering transaction and are therefore subject to forfeiture pursuant to pursuant to 18 U.S.C. § 981(a)(1)(A).

63. I also have probable cause to believe that the seized $1,098,699.64 constitutes proceeds traceable to a violation of 18 U.S.C. § 1343 and/or 18 U.S.C. § 1349, and are therefore is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

As provided in 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Brad Schley, Special Agent
U.S. Secret Service